

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-215590

(43)Date of publication of application : 02.08.2002

(51)Int.Cl. G06F 15/00
G06F 1/00
G06K 17/00
G06K 19/10
H04L 9/32

(21)Application number : 2001-009771

(71)Applicant : TDK CORP

(22)Date of filing : 18.01.2001

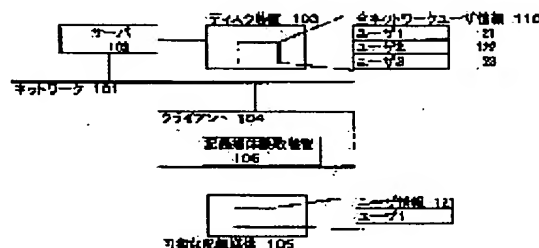
(72)Inventor : TSUNEKAWA HARUKI

(54) RECORDING MEDIUM FOR NETWORK LOG-IN AND NETWORK LOG-IN METHOD USING THE SAME

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a network log-in method which is convenient and protected against illegal use by using a portable recording medium for network log-in.

SOLUTION: User information is divided and recorded on a plurality of portable recording media for network log-in. Log-in operation is done by using the portable recording media and user information is ciphered to attain protection against illegal use. The user information is rewritten to the portable recording media at log-out time to make the security to the illegal use higher.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

the examiner's decision of rejection or
application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-215590
(P2002-215590A)

(43) 公開日 平成14年8月2日 (2002.8.2)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 G 5 B 0 3 5
1/00	3 7 0	1/00	3 7 0 E 5 B 0 5 8
G 0 6 K 17/00		G 0 6 K 17/00	T 5 B 0 8 5
19/10		19/00	R 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 C

審査請求 未請求 請求項の数4 O L (全 5 頁) 最終頁に続く

(21) 出願番号 特願2001-9771(P2001-9771)

(22) 出願日 平成13年1月18日 (2001.1.18)

(71) 出願人 000003067

ティーディーケー株式会社

東京都中央区日本橋1丁目13番1号

(72) 発明者 常川 春樹

東京都中央区日本橋一丁目13番1号 ティーディーケー株式会社内

Fターム(参考) 5B035 AA14 BB09 BC01 CA38

5B058 CA27 KA02 KA04 KA08 KA31

KA35 YA20

5B085 AE02 AE11 AE29

5J104 AA07 AA12 AA16 EA03 EA13

KA01 NA02 NA05 NA27 NA30

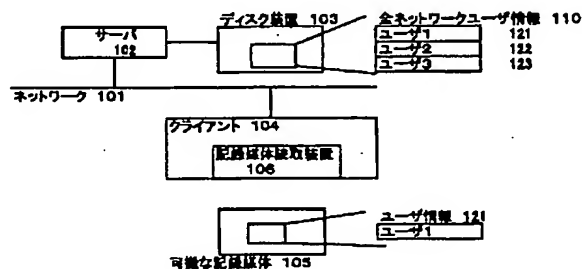
NA36 PA07

(54) 【発明の名称】 ネットワークログイン用記録媒体及びそれを用いるネットワークログイン方法

(57) 【要約】 (修正有)

【課題】 ネットワークログイン用の可搬な記録媒体を用いて簡便でかつ不正使用から保護されたネットワークログインの方法を提供する。

【解決手段】 ネットワークログイン用の複数の可搬な記録媒体にユーザ情報を分割して記録しておく。この複数の可搬な記録媒体によりログインを行うとともに、ユーザ情報を暗号化することにより不正使用から保護する。またログアウトするときに当該ユーザ情報を当該可搬な記録媒体上に書き換えることにより不正使用に対する安全性をより一層高める。



【特許請求の範囲】

【請求項1】 ネットワークログインに必要なユーザ情報が分割して記録されていることを特徴とする複数枚の可搬な記録媒体。

【請求項2】 上記可搬な記録媒体上に記録された上記ユーザ情報は公開鍵暗号方式で暗号化されていることを特徴とする、請求項1記載の記録媒体。

【請求項3】 上記ユーザ情報はログアウトするときに上記ユーザ情報を書き換えることができることを特徴とする、請求項1又は請求項2に記載の記録媒体。

【請求項4】 請求項1乃至3記載の記録媒体によりネットワークに接続するネットワークログイン方法

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、ネットワークにログインする際に使用する記録媒体及びログイン方法に関する。

【0002】

【従来の技術】 ネットワークにログインするには、ログインするユーザはあらかじめ登録しておいたパスワードを用いて、キーボードより入力される正しいパスワードによって正しいユーザーとして認証され、ネットワークにログインするのが通常の方法である。しかしながら、ログインすることにパスワードをキーボードから入力するのはユーザの利便性に欠ける。またパスワードを忘れてしまっても正しいユーザであるにもかかわらず、ログインできない、あるいは、他人にパスワードを盗まれて不正にログインされてしまう、等の問題があった。そこで特開平3-268050号公報、特開平6-348650号公報に記載のように、ユーザ情報、パスワードなどからなるログイン情報を可搬な記録媒体上に記録しておき、該可搬な記録媒体を用いてログインする方法が考えられていた。

【0003】

【発明が解決しようとする課題】 上記のような可搬な記録媒体を用いてネットワークにログインする手段だけでは、可搬な記録媒体を使用するがためにこの記録媒体を不正に入手した者による不正なログインを完全に防止することはできなかった。

【0004】

【課題を解決するための手段】 上記のような課題を解決するため、本発明では可搬な記録媒体をもちいてネットワークにログインする手段としての該可搬な記録媒体を複数枚とすること、該記録媒体に記録する情報は公開鍵暗号方式で暗号化されていること、該情報はログアウトする毎に該可搬な記録媒体に再記録されることにより常に最新の情報に保たれること、などにより上記可搬な記録媒体を第三者が入手して不正にログインすることを防止できる手段を提供するものである。

【0005】

【作用】 可搬な記録媒体を用いてネットワークに自動的にログインする手段により、ネットワークの1クライアントPCからネットワークにアクセスするとともに、該可搬な記録媒体の不正使用を防止する。

【0006】

【実施例】 本発明の1実施例について図1を用いて説明する。

【0007】 図1を用いて、可搬な記録媒体上にあるユーザのログイン情報をもとに、ネットワークへ自動的にアクセスを開始する（以後これをログインと呼ぶ）原理を説明する。

【0008】 101はネットワーク、102はネットワーク（101）のサーバ、103はサーバ（102）に接続されているディスク装置、104はネットワーク（101）のクライアントPC、105はクライアントPCにより情報を読み書き可能な可搬な記録媒体、106はクライアントPC（104）に接続されている記録媒体読取装置である。本実施例では説明簡略化のため、サーバ（102）、クライアントPC（104）は各1つとなっているが、これらはネットワーク（101）上に複数あってもかまわない。

【0009】 ディスク装置（103）に保管されている、該サーバ（102）を用いている全ネットワークユーザ情報、121は可搬な記録媒体（105）内にあり、ユーザ情報である。

【0010】 さらに、全ネットワークユーザ情報（110）にはネットワークユーザとしてユーザ1（121）、ユーザ2（122）、ユーザ3（123）に関するユーザ情報が記録されており、可搬な記録媒体（105）内にはユーザ1（121）一人分のログイン情報が記録されている。このような構成をもつネットワーク（101）において、ネットワークユーザであるユーザ1（121）が、自身のログイン情報が記録されている可搬な記録媒体（105）を、ネットワーク（101）上のクライアントPC（104）内にある記録媒体読取装置（106）に装着すると、クライアントPC（104）は可搬な記録媒体（105）内のユーザ情報（121）を読み、ログイン情報をサーバ（102）に送る。サーバ（102）は接続されているディスク装置（103）内にある全ネットワークユーザ情報（110）と照合してこのログイン情報が正しいければ、ユーザ1（121）を認証して、ネットワーク（101）を利用することを許可する。もしも、前記ユーザ情報（121）と全ネットワークユーザ情報（110）との照合が正しくなければ、ユーザ1（121）は認証されずネットワーク（101）にログインできないためネットワークの利用をすることはできない。

【0011】 図1では便宜上可搬な記録媒体にユーザ情報すべてを記録してあるものとして説明したが、本発明はユーザ情報が複数枚の記録媒体に分割されていること

に特徴がある。以下、図2及び図3を用いてこれを説明する。

【0012】ユーザ情報(121)は図2に示すように、ユーザの名前、ID番号、パスワード、ユーザのアクセスレベル、ユーザとして許される期限、などから構成される。このユーザ情報(121)を図1では可搬な記録媒体(105)のなかに一括して記録してあるものとして説明したが、一部づつ複数の媒体に分ける。ここでは可搬な媒体を2枚用いる例を図3により説明する。

ユーザ情報(121)は2枚の可搬な媒体(105aと105b)のなかにユーザ情報a(121a)とユーザ情報b(121b)とに分かれて記録されている。まず第一の可搬な媒体(105a)を図1と同様にクライアントPC(104)に接続されている記録媒体読取装置(106)に装着するとクライアントPC(104)は可搬な記録媒体(105a)内のユーザ情報の一部(121a)を読む。クライアントPC(104)はサーバ(102)に読み取ったユーザ情報(121a)を送る。サーバ(102)は全ネットワークユーザ情報(110)中のユーザ情報(121から123)を調べるがユーザ情報の一部(121a)しかないためユーザ情報(121)を構成できずログインが許可されないことをクライアントPCに伝える。ここでユーザはもう一枚の可搬な記録媒体(105b)をクライアントPC(104)に接続された記録媒体読取装置(106)に装着すると、クライアントPC(104)は可搬な記録媒体(105b)よりユーザ情報の残りの部分(121b)を読む。クライアントPC(104)はサーバ(102)に2枚目の可搬な記録媒体(105b)から読み取ったユーザ情報(121b)を送る。サーバ(102)は全ネットワークユーザ情報(110)中のユーザ情報(121から123)を調べ、全てのユーザ情報(121)が構成されていることを知るのでログインを許可する。

【0013】このようにしてログイン情報を2枚の可搬な記録媒体に分割して記録することにより悪意ある第三者がこの可搬な記録媒体を不正に入手しようとしても2枚を入手する必要がある、1枚のときよりも著しく不正に使用される危険が減少していることは言うまでもない。また3枚以上に分割すれば不正に使用される危険はより減少する。

【0014】ユーザ情報(121)の分割の方法としてユーザ情報(121)の構成要素であるユーザの名前、ID番号、パスワード、ユーザのアクセスレベル、ユーザとして許される期限、などの項目を分割して記録してもいいし、パスワードの上位桁、下位桁のように項目内で分割して記録しても効果は同じように期待される。

【0015】図4を用いてユーザ情報の暗号化について説明する。

【0016】悪意ある第三者がユーザ情報(121)の

記録された可搬な記録媒体を不正に入手し、ユーザ情報(121)を改ざんして使用することがある。例えばより機密性の高い情報にアクセス可能となるべく、ユーザアクセスレベルを通常レベルからより高い管理者レベルに改ざんしたり、アクセス可能期限がきれているにもかかわらず、期限情報を改ざんしてアクセスを可能としたりする場合が予想される。改ざんを防止するには、上記可搬な記録媒体内のユーザ情報(121)を容易に読むことができないように、暗号化を施せばよい。ただし、通常の暗号化では、暗号化のための「鍵」をサーバ(102)とクライアントPC(104)が共有するため、「鍵」の秘匿管理を十分行う必要がある。ましてネットワーク上のように多くの人に公開された場であると「鍵」をネットワークでサーバ(102)とクライアントPC(104)の間で送受するときに、傍受されてしまう危険性もある。

【0017】そこで、この暗号化の手法として「公開鍵暗号方式」をもちいてユーザ情報(121)を暗号化しておけばよい。「公開鍵暗号方式」としてはRSA方式が著名である。RSA暗号方式については、例えば文献「情報セキュリティの科学」BLUEBACKS P130〜に述べられている。最初にサーバ(102)はクライアントPC(104)との間にRSA方式による「秘密鍵」(141)「公開鍵」(142)を定め、クライアントPC(104)には「公開鍵」を提示する。クライアントPCはこの「公開鍵」を用いて、ユーザ情報(121)を暗号化する。クライアントPC(104)はこの暗号化されたユーザ情報(121E)をサーバ(102)に送る。サーバ(102)は「秘密鍵」により暗号化されたユーザ情報(121E)を解き、全ネットワークユーザ情報(110)と比較して、ログインの可否を決める。

【0018】図5を用いてログアウトするとき上記可搬な記録媒体上にユーザ情報(121)を書き換えることについて説明する。なお、ログアウトとはユーザがネットワークからの接続を切って離れることをいう。

【0019】上記「公開鍵暗号方式」にて暗号化されたユーザ情報であるが、悪意ある第三者からの情報保護のうえでは、暗号の鍵を時々更新するのが望ましい。本発明ではこれをログアウトするときに更新し、ユーザ情報(121)の保護を図っている。ユーザがログアウトするときは、サーバ(102)は新たな「秘密鍵」と「公開鍵」を作成する。

【0020】サーバ(102)は接続されているディスク装置(103)に保管されている全ネットワークユーザ情報(110)より、当該ログアウトするユーザ情報(ここではユーザ1を例として説明する)(121)を取り出し、ネットワーク(101)を経由してクライアントPC(104)に送る。このときサーバ(102)は新たに作成した「公開鍵」(142)もクライアントPC(104)に送る。クライアントPCはこのユーザ情報

(121)を当該「公開鍵」(142)にて暗号化し、クライアントPCに接続されている記録媒体書き込み装置(107)に挿着された可搬な記録媒体(105)に暗号化されたユーザ情報(121e)として記録する。

【0021】

【発明の効果】可搬な媒体を用いてログインするため正規ユーザにはキー入力時の負担を減らすことができ、さらに暗号化された複数の媒体を用いることによる、第三者の不正なログインを防止することができる。

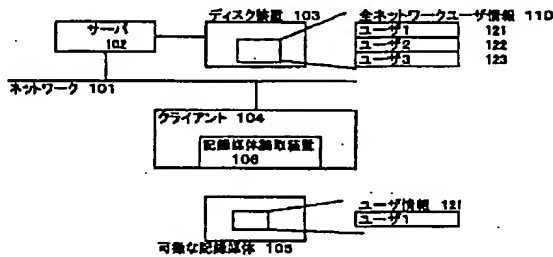
【図面の簡単な説明】

【図1】可搬な記録媒体上のユーザ情報を用いてネットワークにログインする原理図である。

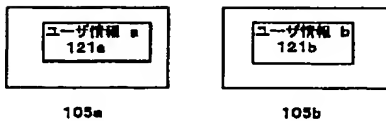
【図2】ユーザ情報の内容の例を示す図である。

【図3】ユーザ情報が分かれて記録された複数の可搬な記録媒体の図である。

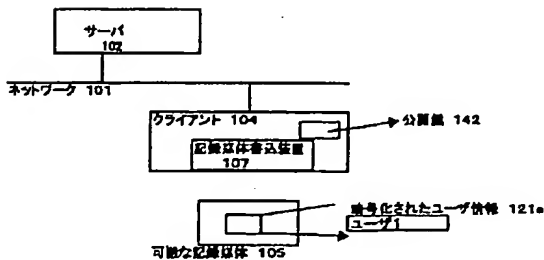
【図1】



【図3】



【図5】



*【図4】ユーザ情報の暗号化を行う原理図である。

【図5】ユーザ情報をログアウト時に可搬な記録媒体に書き込む原理図である。

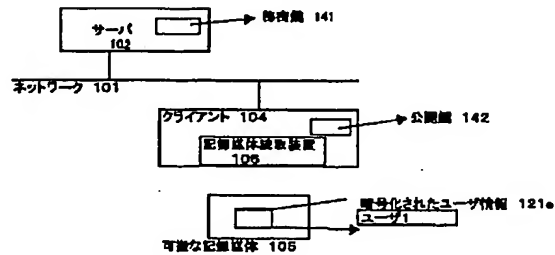
【符号の説明】

101…ネットワーク、102…サーバ、103…ディスク装置、104…クライアントPC、105…可搬な記録媒体、105a…第一の可搬な記録媒体、105b…第二の可搬な記録媒体、106…記録媒体読取装置、107…記録媒体書き込み装置、110…全ネットワークユーザ情報、121…ユーザ情報、121a…第一の可搬な記録媒体に記録されている一部のユーザ情報、121b…第二の可搬な記録媒体に記録されている一部のユーザ情報、121e…暗号化されたユーザ情報、121から123…各ユーザ情報、141…暗号化のための秘密鍵、142…暗号化のための公開鍵

【図2】

ユーザ情報 121	
ユーザ名	ユーザ1
ID	ABCD
パスワード	1234
ユーザアクセスレベル	通常
期限	2001/12/31
その他の情報	なし

【図4】



(5)

特開2002-215590

フロントページの続き

(51)Int.Cl.⁷

識別記号

F I
H 0 4 L 9/00

ターマード (参考)

6 7 3 E